The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

05/21/2014

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Google Chrome versions prior to 35.0.1916.114

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been reported in Google Chrome. Details of the vulnerabilities are as follows:

- A use-after-free vulnerability exists in styles. [CVE-2014-1743]
- An integer-overflow issue exists in audio. [CVE-2014-1744]
- A use-after-free vulnerability exists in SVG. [CVE-2014-1745]
- An Out-of-bounds read issue exists in media filters. [CVE-2014-1746]
- An UXSS (universal cross-site scripting) issue exists in local MHTML file. [CVE-2014-1747]
- An UI spoofing issue exists in scrollbar. [CVE-2014-1748]
- Multiple security vulnerabilities exist due to an unspecified error. [CVE-2014-1749]
- An integer-underflow issue exist due to an unspecified error in the V8 Javascript engine. [CVE-2014-3152]

These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

REFERENCES:

Google:

http://googlechromereleases.blogspot.com/2014/05/stable-channel-update_20.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1743

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1744

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1745

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1746

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1747

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1748

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1749

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3152

SecurityFocus:

http://www.securityfocus.com/bid/67517